

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Norfolk Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
INSTAGRAM ACCOUNTS **jlincon.va**
(628135413) and **jesslincon06 (56518767617)**
THAT IS STORED AT PREMISES
CONTROLLED BY META PLATFORMS,
INC.

Case No. 2:24-SW- 144

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Matthew E. Lee, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with two Instagram accounts – **jlincon.va (628135413)** and **jesslincon06 (56518767617)** (hereinafter, the “TARGET ACCOUNTS”) -- that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), an electronic communications service and/or remote computing service provider headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and I have been so employed since 2017. I am currently assigned to the Washington Field Office's Child Exploitation and Human Trafficking Task Force located at the Northern Virginia Resident Agency. As a Special Agent, I investigate federal violations concerning kidnapping, child pornography, the sexual exploitation of children, human trafficking, and related offenses. I have gained experience through training and work related to conducting these types of investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251(a)/(e) (sexual exploitation/attempted sexual exploitation of minors), 2422(b) (coercion and enticement/attempted coercion and enticement of minors), and 2252(a)(4)(B)/(b)(2) (possession of material involving the sexual exploitation of minors) have been committed by GARY OWENS JR. ("OWENS"). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND CONCERNING INSTAGRAM¹

6. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510.

Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the TARGET ACCOUNTS, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

7. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

8. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

9. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the

¹ The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Privacy Policy," <https://privacycenter.instagram.com/policy/>; "Information for Law Enforcement," <https://help.instagram.com/494561080557017>; and "Help Center," <https://help.instagram.com>.

primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

10. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

11. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

12. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user’s devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

13. Each Instagram user has a profile page where certain content they create and share (“posts”) can be viewed either by the general public or only the user’s followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography (“Bio”), and a website address.

14. One of Instagram’s primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users (“tag”), or add a location. These appear as posts on the user’s profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta’s servers.

15. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can “mention” others by adding their username to a comment followed by “@”). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

16. An Instagram “story” is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator’s “Stories Archive” and remain on Meta’s servers unless manually deleted. The usernames of those who viewed a story are visible to the story’s creator until 48 hours after the story was posted.

17. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are

removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

18. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

19. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

20. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Meta retains records of a user's search history and followed hashtags.

21. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

22. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

23. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

24. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

25. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to

establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

26. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, voice messages, photos, and videos are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. For example, as described further below, multiple minor victims in this case have stated in interviews with the FBI that someone used an Instagram account to initially contact them before directing them to the Kik messaging application where the crimes described below were committed.

27. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

28. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account

may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, associated and linked accounts, stored communications, photos, and videos may reveal services used in furtherance of the crimes under investigation. In addition, stored communications, contact lists, photos, and videos can lead to the identification of additional victims, co-conspirators, and instrumentalities of the crimes under investigation.

30. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND ON KIK

16. As described below in greater detail, in addition to Instagram, OWENS used the messaging application "Kik" to communicate with numerous minors. According to Kik's website, Kik is an application that lets users "*connect with friends and groups from all around the world through messaging, chatting and live streaming.*" Kik users can exchange text, images, videos, and more with Kik's messenger function.

17. Kik offers users the ability to create an identity within the app referred to as a username. This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account to obtain a different username. The username for a particular Kik account holder is displayed in their Kik profile.

18. I know, based on my training and experience, that individuals who use the Internet to sexually exploit children often use Kik because of the perceived anonymity of the Kik application. For example, according to Kik's website, "*as a security measure, when you log out of your account, your chat messages are automatically cleared. Once you log in again, your contacts and list of chats in your main chat list will appear as you left them before logging out.*"

PROBABLE CAUSE

27. On or about July 27, 2022, the social media company Meta submitted information to the National Center for Missing and Exploited Children (NCMEC) regarding the potential extortion of a minor (hereafter, "Minor Victim 1" or "MV1") on Instagram. NCMEC compiled this information into a CyberTip ("CT") Report and provided the FBI with pictures of MV1 that were associated with the potential extortive conversation.

28. On or about December 9, 2022, I interviewed Minor Victim 1's parents -- B.P. and R.P. -- who confirmed that the person in one of the pictures associated with the CT Report was their child, MV1. At the time of this interview, MV1 was 17 years old. Additionally, at all times relevant to the facts in this affidavit, B.P., R.P., and MV1 lived in Gainesville, Virginia, which is in the Eastern District of Virginia.

29. On or about December 12, 2022, R.P. and B.P. provided their consent for the FBI to search MV1's phone and provided the phone to the FBI. Later that same day, FBI personnel extracted the digital contents of the phone for my further review.

30. While reviewing MV1's phone, I located a conversation between MV1 and another user on Kik, which occurred on or about October 31, 2022. This conversation was unrelated to the attempted extortion of Minor Victim 1 as reported in the CT Report.

31. The username of the person with whom MV1 communicated on Kik was “misslincon.” As described in more detail below, I believe OWENS was the person controlling this account while posing as a female close in age to MV1. However, OWENS is a male and was 40 years old at the time of this conversation. Minor Victim 1 was 17 years old at the time of this conversation. Relevant portions of the conversation are transcribed below.²

Minor Victim 1: *hey*

Misslincon: *hey wyd bby*

Minor Victim 1: *nothin*

Minor Victim 1: *u go first ok bby*

Misslincon: *what you got on bby*

Minor Victim 1: *nothing*

Minor Victim 1: *wbu*

Misslincon: *you're lying*

Minor Victim 1: *well i got underwear on but like basically nothing*

Misslincon: *lemme see*

32. At “misslincon’s” direction, MV1 sent a picture to “misslincon,” which shows his legs and the bottom of his torso as he appears to be under a blanket. In the picture, MV1’s underwear is shown. The conversation then continued as follows:

Misslincon: *want me to suck you*

Minor Victim 1: *yes*

Misslincon: *make it move krnmrcseee*

² All quotations transcribed herein are provided verbatim as in the original including all errors.

Misslincon: *lemme see*

Minor Victim 1: *u gotta send something first*

33. “Misslincon” then sent a picture to MV1. The picture shows a nude white female on her knees facing the camera as the female leans forward and rests on her elbows. The photo shows a portion of the female’s face, her back, and her bare buttocks. In the picture, the female’s chest is close to the ground as she leans forward. The conversation then continued as follows:

Misslincon: *uh huh*

Minor Victim 1: *hot asf*

Misslincon: *make it move bby*

Minor Victim 1: *its not hard enough yet u gotta send me ur tits or something*

Misslincon: *get me wetter lemme see you head to toe laying in bed in undies on video*

34. At “misslincon’s” direction, MV1 sent a video to “misslincon.” I have reviewed this video in its entirety. The video, which lasts approximately four seconds, shows a male’s body with underwear on as the male lies on what appears to be a bed. The blankets and the underwear shown in this video appear to match the blankets and underwear shown in the picture MV1 had previously sent to “misslincon.” The conversation then continued as follows:

Misslincon: *you wanna fuck me bby*

Minor Victim 1: *yes ofc*

Misslincon: *raw or no*

Minor Victim 1: *u wanna fuck me?*

Minor Victim 1: *and raw fs*

Misslincon: *yes bby*

Misslincon: *take ur undies off lemme watch idc if if it’s soft we will make it hard*

Minor Victim 1: *ok bby*

35. Again, in response to the direction provided by “misslincon,” MV1 sent a video to “misslincon.” The video, which I have reviewed in its entirety, lasts approximately eight seconds and appears to show the same male as described above. In this video, the male removes his underwear, thus exposing his erect penis to the camera. The conversation then continued as follows:

Minor Victim 1: *alr now i need to see some of that wet pussy*

Misslincon: *mmm bby lemme see you jerk it*

Minor Victim 1: *pussy first i gotta have something to jerk to*

36. “Misslincon” then sent another picture to MV1. This picture shows a nude white female. In the picture, the female is standing in front of the camera while facing away from the camera and bending over slightly at the waste, thus exposing her bare buttocks and vagina to the camera. The female in the picture is standing in front of a mirror, with her reflection also visible to the camera. The female’s reflection shows her bare breasts and her mouth open with her tongue out of her mouth. The conversation then continued as follows:

Misslincon: *like this bby*

Minor Victim 1: *yes bby ur so hot*

Misslincon: *jerk it bby lemme watch*

37. Once again, at the direction of “misslincon,” MV1 sent a video. I have reviewed this video in its entirety. The video, which lasts approximately seven seconds, shows a male using his hand to masturbate his erect penis. Based on the background in the video, including the blankets on the bed, I believe the male in this video is the same person shown in the video

and picture that MV1 had previously sent as described above. The conversation then continued as follows:

Minor Victim 1: *let me see u finger urself*

Misslincon: *mmmmm you're huge bby*

Minor Victim 1: *thank you bby*

Minor Victim 1: *u still there?*

Misslincon: *my mom woke up*

Misslincon: *hang on a bit*

Minor Victim 1: *just be quiet*

Minor Victim 1: *send me something*

Misslincon: *I am being quiet but i gotta chill*

Minor Victim 1: *nah send something bruh*

Misslincon: *bro you want me to get caught on this too haha*

Minor Victim 1: *no but like just be quiet its not hard*

Misslincon: *yeah but she can walk in my room any minute to see what i'm doing*

Minor Victim 1: *why would she tho*

Misslincon: *bro cuz she's caught me sending before lol*

Minor Victim 1: *ok but like just be quick with it*

Minor Victim 1: *listen so u stop if shes coming*

Misslincon: *bro lol you'll get one more*

Minor Victim 1: *ok*

38. “Misslincon” then sent another picture to MV1. This picture shows a nude white female with her breasts and torso exposed. A small portion of the female’s face and the top of her pubic area can be seen in the picture. The conversation then continued as follows:

Misslincon: *i wanna feel you inside me*

Minor Victim 1: *i wanna be inside of u bby*

Misslincon: *me too will you cum in me*

Minor Victim 1: *yes ofc bby*

Minor Victim 1: *we should meet up sometime and do it*

Minor Victim 1: *u make me so horny*

Misslincon: *that would be hot babe*

Minor Victim 1: *oh yea fs*

Misslincon: *you gonna cum*

Minor Victim 1: *i did bc i got on the hub³*

Minor Victim 1: *since u left*

Misslincon: *how was it*

Minor Victim 1: *good fs*

Misslincon: *is it still there can i see it*

Minor Victim 1: *sure*

Misslincon: *ok*

³ Based on training and experience and the context of this conversation, I believe Minor Victim 1 said “the hub” in reference to a popular pornography website, Pornhub.

39. At “misslincon’s” direction, MV1 sent another picture. This picture shows a red and blue towel with a white liquid on it. Based on the context of the conversation, I believe the liquid on the towel is MV1’s semen. The conversation then continued as follows:

Misslincon: *damn you ever cum on your chest babe*

Minor Victim 1: *yea i have*

40. On or about January 6, 2023, an FBI child adolescent forensic interviewer interviewed Minor Victim 1. During that interview, MV1 discussed the conversation with “misslincon.” Minor Victim 1 advised that “misslincon” was someone he met online approximately two years before the interview. Minor Victim 1 was 17 years old at the time of this interview and was approximately 15 years old at the time he met “misslincon” online.

41. Minor Victim 1 advised that he knew the user of the “misslincon” Kik account as “Jessica Lincon.” Minor Victim 1 also advised that, although he could not remember on what platform he initially met “Lincon,” he had communicated with her on Instagram and Kik.

42. During the forensic interview, MV1 advised that he believed “Lincon’s” Instagram account username was her name, “Jessica Lincon,” with a period or underscore somewhere in the username. As described above, the usernames for the TARGET ACCOUNTS are jlincon.va and jesslincon06, consistent with MV1’s description of “Lincon’s” Instagram account username.

43. Minor Victim 1 advised that he did not remember the exact point at which his relationship with “Lincon” turned sexual, but eventually they got to the point where they would simply contact each other and request sexual content. During the interview, MV1 identified himself in screenshots taken from the videos he sent in the conversation described above,

including a screenshot from the video in which MV1 masturbated his penis with his hand. Minor Victim 1 advised that he only sent this video to “Lincon.”

44. In October 2023, a member of the FBI’s Child Exploitation and Human Trafficking Task Force (CEHTTF) identified the individual in the pictures sent by “misslincon” to MV1 as an individual identified herein as JANE DOE. The investigation has revealed that content of JANE DOE can be found on various pornography websites. The content of JANE DOE on these websites appears visually similar to the Kik profile picture for “misslincon.”

45. A member of the CEHTTF was then able to fully identify JANE DOE as a woman who, in October 2022 (*i.e.* when Kik user “misslincon” communicated with MV1 as described above), was 21 years old. JANE DOE is originally from New York, and in October 2023, JANE DOE lived in Florida. As described in more detail below, the “misslincon” Kik account was accessed on multiple occasions from IP addresses that resolved to the Southeast Virginia area. The CEHTTF has identified no information that indicated JANE DOE has ever lived in Southeast Virginia. Based on my training and experience and these facts as well as additional facts learned in the investigation set forth below, the person using the “misslincon” Kik account (*i.e.*, OWENS) was using JANE DOE’s publicly available photos to “catfish”⁴ MV1.

Identification of Owens

46. On or about December 29, 2022, a member of the CEHTTF served an administrative subpoena on Kik for records associated with the Kik user “misslincon.”

⁴ According to dictionary.cambridge.org, “catfishing” is “the practice of pretending on social media to be someone different, in order to trick or attract another person.”

According to the records provided by Kik in response, on or about December 14 and 15, 2022, the “misslincon” Kik account was accessed from the IP address 72.214.52.41.

47. On or about January 5, 2023, a member of the CEHTTF served an administrative subpoena on Cox Communications for subscriber records associated with this IP address.

According to the records provided by Cox Communications in response, the IP address 72.214.52.41 was assigned to the Courts at Yorkshire, LLC with an address of 101 Little Bay Avenue, Yorktown, Virginia 23693. This address is within the Eastern District of Virginia.

48. The Courts at Yorkshire, VA is an apartment complex. Because the IP address 72.214.52.41 was assigned to the entire apartment complex and not a particular resident within the complex, the FBI was not able to identify the user of the “misslincon” account based on this information alone.

49. Accordingly, on or about September 13, 2023, a member of the CEHTTF served an administrative subpoena on Kik for updated records and IP logs associated with the “misslincon” Kik account. According to the records provided by Kik in response, the “misslincon” Kik account was accessed from the IP address 75.249.216.181 at 11:12pm UTC. Additionally, on or about August 22, 2023, the “misslincon” Kik account was accessed from the IP address 75.249.216.181 at 4:21am UTC⁵.

50. On or about September 20, 2023, a member of the CEHTTF served an administrative subpoena on Verizon for records associated with this IP address. According to the records provided by Verizon in response, at 11:12pm on August 20, 2023, and at 4:21am on August 22, 2023, the IP address 75.249.216.181 was assigned to OWENS at 7243 Arrington

⁵ UTC stands for Coordinated Universal Time.

Street, Unit D, Suffolk, Virginia 23435. This is the same address listed on OWENS' Virginia driver's license, and it is within the Eastern District of Virginia.

51. After obtaining this information, a member of the CEHTTF began investigating OWENS' online presence, including his LinkedIn profile.⁶ Specifically, on or about October 17, 2023, a member of the CEHTTF accessed LinkedIn and located a profile for OWENS. The profile indicated that OWENS was the Assistant Property Manager at the Courts at Yorkshire Downs.

Search of OWENS' Residence and iPad

52. On February 29, 2024, the Honorable United States Magistrate Judge Ivan D. Davis of the Eastern District of Virginia issued a search warrant for OWENS' person, residence, and vehicle. On March 5, 2024, FBI personnel (including your affiant) executed the search warrant on OWENS' residence, person, and vehicle. During the execution of this search warrant, several digital devices, including an iPad, were seized. I also briefly interviewed OWENS.

53. FBI personnel used a forensic tool to extract the contents of the iPad for my further review. While reviewing this data, I identified several items that indicated that the iPad belonged to OWENS. For example, some of the messages contained in the iPad were from Facebook Messenger. The account display name for the messages sent from the iPad was "Gary Owens Jr." Additionally, information for two credit cards was stored on the iPad. The name on both of these cards was "Gary Owens Jr." Finally, the Apple ID associated with the iPad was the email address thehazardoflove@aol.com. During my review of the iPad, I found numerous

⁶ LinkedIn is a website on which people create profiles detailing their professional experiences and employment information, typically for professional networking purposes.

emails to this email address, including one sent on or about February 25, 2024, from orders@eat.grubhub.com. This email stated, in relevant part, “*ETA 10:51 AM to 7243 Arrington St., Suffolk, VA Thank you for ordering, Gary Owens.*” As described above, the 7243 Arrington Street address is OWENS’ residence. Accordingly, I submit there is probable cause to believe the iPad discussed herein belonged to OWENS.

54. OWENS’ iPad was manufactured in China. During my review of OWENS’ iPad, I conducted a physical examination of the device. The text on the back of OWENS’ iPad reads, “*Designed by Apple in California. Assembled in China.*” Accordingly, I submit there is probable cause to believe OWENS committed the acts described herein while using an iPad that was assembled outside of the United States and is therefore a facility of foreign commerce.

55. Also during my review of the data extracted from the iPad, I located the Kik application. Within the Kik application, I identified more than 300 Kik conversations, most of which had been deleted but subsequently recovered by the forensic tool used to extract the data from the iPad. I reviewed each of these conversations. Based on my review, I identified numerous conversations in which the operator of the iPad (whom I believe to be OWENS) posed as JANE DOE while communicating with males who appear to be minors.

56. During this review, I also located several items associated with JANE DOE. For example, I found an undated Google search for “Jessica stardust” and internet history that indicated the user of the iPad navigated to a page of nudostar.com,⁷ which was titled, “Others – JANE DOE.”⁸ Another web history item indicated the user of the iPad navigated to

⁷ Nudostar.com is an adult pornography website.

⁸ The redacted name, JANE DOE, is the real name of Jessica Stardust.

pornpic.xxx/user/jessicastardust. Finally, I found information associated with the Kik user account “misslincon,” along with a password that OWENS also used for other accounts on the iPad.

57. OWENS’ iPad had many applications installed on it. One of those applications was “Calculator%,” which is an application whose icon on the iPad screen appears to indicate that the application is a normal calculator. However, this application is actually used to store files, including pictures and videos. I know, based on training and experience, that people who have a sexual interest in minors often use applications like this one to hide their child pornography files. When FBI personnel accessed this application on OWENS’ iPad, six folders inside the application were located. These folders were entitled, “Jessica,” “2019,” “2020,” “2021,” “2022,” and “2023.”

58. I reviewed the “Jessica” folder in the Calculator% application on OWENS’ iPad and identified approximately 207 files, including pictures and videos. Most of these files show JANE DOE in some stage of undress or engaged in a sex act. Some of these files appear to be the same files that OWENS had previously sent to MV1 while OWENS catfished MV1. Based on this information, I believe the “Jessica” folder was OWENS’ cache of files he used while catfishing minors as JANE DOE.

59. I also reviewed the “2022” folder in the Calculator% application on OWENS’ iPad and identified approximately 904 files, including pictures and videos. Most of these files show males in some stage of undress or engaged in a sex act, including masturbation. Within these 904 files, I found several pictures and videos of MV1, including videos in which MV1 uses his hand to manipulate his penis while his underwear is still on. Based on this information, I

believe the “2022” folder is the folder in which OWENS maintained the pictures and videos he obtained in the year 2022 from his catfishing scheme.

60. The “2019,” “2020,” “2021,” and “2023” folders contained similar content as the “2022” folder. Accordingly, I believe OWENS created folders that correlated to the years he conducted this scheme and that he maintained the pictures and videos he obtained in those years in the corresponding folder within the Calculator⁹ application.

61. One of the Kik conversations I found on OWENS’ iPad was his conversation with MV1. The Kik conversation between MV1 and OWENS on OWENS’ iPad contained more data than the version I found on MV1’s phone. Specifically, the conversation on OWENS’ iPad began on February 20, 2022, and ended on October 31, 2022.⁹ In February 2022, when this conversation began, MV1 was 16 years old.

62. On May 21, 2024, United States Magistrate Judge Robert J. Krask signed a complaint in which OWENS is charged with (1) the sexual exploitation and attempted sexual exploitation of children, in violation of 18 U.S.C. § 2251(a) and (e); and (2) the coercion and enticement, and attempted coercion and enticement of a minor, in violation of 18 U.S.C. § 2422(b) as to MV1 (2:24mj86). OWENS was arrested on June 26, 2024.

63. In addition to the conversation between OWENS and MV1, I located many additional chats OWENS had with minors while OWENS catfished them as JANE DOE. Some of those chats are described below.

⁹ The portion of this conversation that occurred on October 31, 2022, and is shown on OWENS’ iPad matches the portion of the conversation that I found on MV1’s phone.

64. Finally, during my review of OWENS' iPad, I located the two Instagram user accounts -- the TARGET ACCOUNTS -- and Instagram direct message conversations involving those two accounts.

Minor Victim 2

65. One of the Kik conversations in OWENS' iPad involved a minor male identified in this investigation as "Minor Victim 2" or "MV2." The Kik conversation between OWENS and MV2 began on December 31, 2021, and ended on September 19, 2022. At the beginning of this conversation, MV2 was 16 years old, and at the end of the conversation he was 17 years old. A relevant portion of this conversation is shown below.

Minor Victim 2: *If we get started now, I'll call you mommy*

OWENS¹⁰: *lol you really wanna do this*

OWENS: *why*

Minor Victim 2: *Yeah let's do it*

Minor Victim 2: *I'm just in that mood*

OWENS: *show me*

66. At OWENS' direction, MV2 sent a media file to OWENS. The thumbnail¹¹ image associated with this file appears to depict a male standing in a bathtub. In the picture, the male's

¹⁰ Based on the information provided above, for the remainder of this affidavit, in transcripts of chats, the "misslincon" Kik account is attributed to OWENS.

¹¹ Because this Kik chat was deleted from OWENS' iPad and then recovered by the forensic tool used to extract the iPad's data, the chat thread itself only contains thumbnail images of media files sent within the chat, even if that media file was a video in the original conversation.

hand is grasping his erect penis. After MV2 sent this file, the conversation continued as shown below.

Minor Victim 2: *This kind of mood*

OWENS: *good boy. More chest and abs*

Minor Victim 2: *Then send something*

OWENS: *you want me from the back*

67. Minor Victim 2 then sent a media file to OWENS. The thumbnail image associated with this file shows a male's bare torso. After MV2 sent this file, the conversation continued as shown below.

Minor Victim 2: *You're damn right I do*

Minor Victim 2: *It's sending*

OWENS: *how deep can you go bby*

OWENS: *ok*

Minor Victim 2: *As deep as you'll let me*

68. Minor Victim 2 then sent a media file to OWENS. The thumbnail of this media file shows a male's hand grasping his erect penis. In response to that file, OWENS said, "*let it flop around lemme admire you.*" At OWENS' direction, MV2 sent another media file. The thumbnail image associated with this file shows a male's erect penis while the male's hand grasps the base of his erect penis. In response to that file, OWENS said, "*no hands bby. be natural.*" Minor Victim 2 then said, "*Send me some of you.*" Then, at OWENS' direction, MV2 sent another media file to OWENS. The thumbnail of this media file shows a male's erect penis with no hands in the picture.

69. Approximately three months later, the Kik conversation between OWENS and MV2 began again. A portion of this conversation is shown below.

OWENS: *show me how you fuck*

Minor Victim 2: *How do you want me to do that*

OWENS: *video bby. fuck ur pillow*

70. At OWENS' direction, MV2 sent another media file to OWENS. The thumbnail associated with this media file shows the tip of a male's penis next to a pillow. After MV2 sent this file, OWENS said, "*lemme see ur balls bby*" and "*lay back open ur legs.*" At OWENS' direction, MV2 sent another media file to OWENS. The thumbnail associated with this file shows a male's legs and scrotum.

71. Approximately three minutes later, OWENS said, "*jerk it more bby.*" At OWENS' direction, MV2 sent another media file. The thumbnail of this media file shows a male's hand grasping his erect penis.

72. A member of the CEHTTF identified MV2 as a now 19-year-old male who lives in Redding, California. On or about May 2, 2024, an FBI Special Agent assigned to the Sacramento Field Office interviewed MV2. During that interview, MV2 confirmed that he was the person in the conversation described above and that he created these files at the direction of the person with whom he was chatting in Kik, whom MV2 believed to be a female.

73. During the interview, MV2 advised that his communications with "Jessica" began when "Jessica" sent him a direct message on Instagram. "Jessica" then suggested that they move their conversation to Kik. Minor Victim 2 advised that he sent several photos and videos to this person in Kik, and four or five of the videos he sent were of him masturbating.

Minor Victim 8¹²

74. One of the Kik conversations in OWENS' iPad involved a minor male identified in this investigation as "Minor Victim 8" or "MV8." The Kik conversation between OWENS and MV8 began on February 22, 2022, and ended on February 24, 2022. At the time of this conversation, MV8 was 15 years old. A relevant portion of this conversation is shown below.

Minor Victim 8: *Anyways can I get a booty pic*

OWENS: *lamo oh fr*

Minor Victim 8: *Bruhaps*

OWENS: *lol you ever sent before*

Minor Victim 8: *Ye*

OWENS: *haha wait how old you is*

Minor Victim 8: *15*

OWENS: *okay me too lol good u a virgin*

Minor Victim 8: *Yes ma'am*

Minor Victim 8: *You?*

OWENS: *nice and i've done a little bit but not much lol have you ever done anything*

...

Minor Victim 8: *Anyways you tryna send*

¹² The minor victim numbers in this affidavit are not consecutive because I have not included all identified minor victims in this affidavit for the sake of brevity. However, minor victim numbers have been and will continue to be used throughout this investigation for various purposes. Accordingly, I have used those constant minor victim numbers for the purposes of consistency throughout this investigation and for later reference.

OWENS: *lol idk if i got in the mood to i could.*

OWENS: *you ever been submissive*

OWENS: *lol*

Minor Victim 8: *Shit maybe like how so*

OWENS: *like i command you to do stuff and you do it and you get rewarded when i say you do good but it's only like for serious ppl lol*

Minor Victim 8: *Lmao kinda like a dog*

Minor Victim 8: *You wanna do that?*

OWENS: *I mean not like a dog but if you want to we can it's up to you*

Minor Victim 8: *Like I'm just trying to see some titties*

OWENS: *lol well you could i just gotta know you're down to have fun too*

Minor Victim 8: *Don't girls like find dick pics gross*

OWENS: *nope haha have u ever sent one before*

75. OWENS continued to talk to MV8 and learned that MV8 was wearing underwear. OWENS then sent a message to MV8 that said, *"lemme see u slide ur undies odd all the way abs then rub ur dock."*¹³ At OWENS' direction, MV8 sent a media file to OWENS. The thumbnail image associated with this file shows a male's torso, groin, and legs while the male's penis is partially protruding beyond the top of the male's grey underwear with green stitching.

76. After reviewing this thumbnail, I performed a manual review of the "2022" folder in OWENS' iPad and located a video file, the beginning frame of which matches the thumbnail

¹³ I believe this message contained several typographical errors. I believe OWENS meant to type *"lemme see u slide ur undies off all the way and then rub ur cock."*

described above. I watched this video, which lasts 10 seconds, in its entirety. In the video, the male pushes his underwear down, thus exposing his entire penis, which is erect. The male then uses his hand to masturbate his erect penis. In the video, a scar can be seen on the male's wrist. After MV8 sent this file, the conversation continued as shown below.

Minor Victim 8: *Don't mind the scar on my wrist I broke my arm and had to have a pin sticking out of it*

OWENS: *i love it tbh*

77. OWENS' conversation with MV8 continued, and MV8 sent additional sexually explicit media files of himself to OWENS.

78. A member of the CEHTTF identified MV8 as a now 17-year-old male who resides in Chesapeake, Virginia, within the Eastern District of Virginia. On June 7, 2024, the same FBI forensic interviewer who interviewed MV1 interviewed MV8. During that interview, MV8 confirmed that he was the person in the conversation described above and that he had sent sexually explicit content of himself to "Jessica." Similar to MV1 and MV2, MV8 advised that he communicated with "Jessica" on Instagram and Kik.

Minor Victim 27

79. One of the Kik conversations in OWENS' iPad involved a minor male identified in this investigation as "Minor Victim 27" or "MV27." The Kik conversation between OWENS and MV27 began on November 17, 2022, and ended on December 18, 2022. At the time of this conversation, MV27 was 16 years old. A relevant portion of this conversation is shown below.

OWENS: *you wanna be my submissive?*

Minor Victim 27: *Idk your asking a lot of someone who's almost a foot taller than you*

OWENS: *that's why i like it :)*

Minor Victim 27: *I guess I can try but no promises*

...

OWENS: *lemme see it how you see it when you look down*

80. Minor Victim 27 then sent a media file to OWENS. The thumbnail of this file, which is shown in the Kik chat thread contained in OWENS' iPad, shows a picture facing down a male's body. The picture shows a male's bare torso, black underwear, bare legs, and white socks. After MV27 sent this picture, the conversation continued as shown below in relevant part.

OWENS: *are you hard bby*

Minor Victim 27: *Nope*

Minor Victim 27: *Not yet*

OWENS: *do you wanna be*

...

OWENS: *do you wanna get a little bit dirtier*

Minor Victim 27: *Sure but only if there's a reward for me*

81. OWENS then sent a picture of JANE DOE to MV27. In this picture, JANE DOE is wearing red lingerie and using a cell phone to take a picture of herself, apparently while facing a mirror. The conversation then continued as shown below in relevant part.

OWENS: *still bulging*

Minor Victim 27: *Yep*

OWENS: *lemme see in video. rub ur bulge*

Minor Victim 27: *Ok for a reward*

OWENS: *soon bby*

82. At OWENS' direction, MV27 sent a media file to OWENS. The thumbnail image associated with this file shows a male's hand above his underwear. Based on the underwear, socks, and background of this thumbnail, I believe the person in this image is the same person as in the image described above.

83. After exchanging several more sexually charged messages with OWENS, MV27 sent a media file to OWENS. The thumbnail image associated with this media file shows a male's erect penis while the male's hand grasps the penis. The conversation then continued as shown below in relevant part.

OWENS: *duck it's so big*

OWENS: *lemme see ur balls and ass bby while ur laying down*

Minor Victim 27: *Ok*

OWENS: *ok bby*

Minor Victim 27: *The ass or the hole?*

OWENS: *hold bby*

OWENS: *hole*

84. Minor Victim 27 then sent a media file to OWENS. The thumbnail image related to this file shows a male's erect penis and a portion of the male's legs. After receiving this file, OWENS asked MV27, "*ever play there*"?

85. Approximately seven minutes later, OWENS sent a message to MV27 that said, "*jerk your cock bby i wanna cum with you*". At OWENS' direction, MV27 sent OWENS a media file. The thumbnail associated with this file shows a male's erect penis with his hand grasping the penis.

86. A member of the CEHTTF identified MV27 as a now 18-year-old male who resides in Moorestown, New Jersey. Minor Victim 27 was 16 years old when OWENS communicated with him via Kik.

87. During my review of OWENS' iPad, I also found Instagram messages between the **jesslincon06 (56518767617)** Instagram account and an Instagram user with a display name identical to MV27's name. All of the Instagram messages between the **jesslincon06 (56518767617)** Instagram account and the other Instagram user, whom I believe to be MV27, occurred on March 13, 2023, which was approximately three months after OWENS' conversation with MV27 on Kik. The conversation is shown below.

MV27: *Nothing*

OWENS: *oh. Well why don't you wanna talk then*

MV27: *I just don't*

OWENS: *oh. not even kik?*

MV27: *Nope*

OWENS: *ok sorry to bother you*

Additional Minor Victims

88. Additional minor victims have been identified and interviewed by the FBI. Several of these minor victims told FBI interviewers that "J[Redacted]" initially contacted them on Instagram before moving the conversation to Kik, where the conversation turned sexual.

89. Additionally, CEHTTF personnel have identified at least two additional potential minor victims (MV14 and MV33), against whom OWENS perpetrated his catfishing scheme on Kik. Minor Victims 14 and 33 have been identified by the FBI, but they have not yet been interviewed. During my review of OWENS' iPad, I found Instagram messaging conversations

between OWENS and other Instagram users with the same names as MV14 and MV33, respectively.

Summary

90. In summary, I submit there is probable cause to believe that OWENS used the TARGET ACCOUNTS to target minor males, whom he subsequently led to the Kik messaging application where he catfished them to persuade them to produce child pornography at his direction and send them to him.

91. As of July 8, 2024, the FBI has identified more than 30 minors against whom OWENS perpetrated this scheme. The FBI is continuing to identify potential additional minor victims.

92. Both of the TARGET ACCOUNTS are variations on the name of OWENS' catfishing persona, Jessica Lincon. Based on my training and experience, I know that catfishing personas are often used exclusively for schemes such as the one described herein. Accordingly, I submit there is probable cause to believe that OWENS used the TARGET ACCOUNTS for the sole purpose of conducting his catfishing scheme for the entire life of the accounts. Accordingly, the requested warrant would require Meta to provide all available data related to the TARGET ACCOUNTS from account opening through account closing or the date of this warrant, whichever is later.

93. On July 8, 2024, your affiant submitted a preservation request to Meta, requesting Meta preserve all data associated with the TARGET ACCOUNTS.

CONCLUSION

31. Based on the forgoing, I request that the Court issue the proposed search warrant.

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Meta. Because the warrant will be served on Meta, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Matthew Lee

Matthew Lee
Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 19th day of July 2024.

Robert J. Krask

UNITED STATES MAGISTRATE JUDGE

Honorable Robert J. Krask
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Instagram accounts **jlincon.va** (Instagram ID 628135413, active on, but not limited to January 29, 2024) and **jesslincon06** (Instagram ID 56518767617, active on, but not limited to February 3, 2024) that are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on July 8, 2024, Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- A. All business records and subscriber information, in any form kept, pertaining to the account, from account opening to closing, including:
 - 1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
 - 2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
 - 3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 - 4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 - 5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
 - 6. Internet Protocol (“IP”) addresses used to create, login, and use the account, including associated dates, times, and port numbers;
 - 7. Privacy and account settings, including change history; and
 - 8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

- B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from account opening to closing;
- C. All content, records, and other information relating to communications sent from or received by the account from account opening to closing, including but not limited to:
 - 1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
 - 2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
 - 3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
 - 4. All associated logs and metadata;
- D. All content, records, and other information relating to all other interactions between the account and other Instagram users from account opening to closing, including but not limited to:
 - 1. Interactions by other Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
 - 2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;
 - 3. All contacts and related sync information; and
 - 4. All associated logs and metadata;
- E. All records of searches performed by the account from account opening to closing; and

- F. All location information, including location history, login activity, information geotags, and related metadata from account opening to closing.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2251(a)/(e) (sexual exploitation/attempted sexual exploitation of minors), 2422(b) (coercion and enticement/attempted coercion and enticement of minors), and 2252(a)(4)(B)/(b)(2) (possession of material involving the sexual exploitation of minors), those violations involving GARY OWENS, JR., including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- A. Child pornography, child erotica, and obscene visual representations of the sexual abuse of children;
- B. Any and all communications regarding child pornography, child erotica, and obscene visual representations of the sexual abuse of children;
- C. Evidence relating to the sexual exploitation of children, including correspondence and communications between the account owner and others on Instagram, as well evidence relating to other social media or third-party platforms that were used for the sexual exploitation of children;
- D. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- E. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- F. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

- G. The identity of the person(s) who communicated with the account holder, in particular individuals who are minors or could be minors, about matters relating to the sexual exploitation and coercion and enticement of minors and the and possession of material involving the sexual exploitation of minors, including records that help reveal their age, identity, and whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.